Guidelines for Managing Trustworthy Digital Public Records Version 2.0

April 2000
Revised July 2013 and October 2013

1 Purpose

To provide guidance to state, county, and municipal government agencies for establishing methods and procedures for creating and maintaining authentic records in digital formats according to the type of records produced and the length of time the records should be retained. These guidelines are designed to ensure the admissibility of an agency's electronic records into evidence in a court of law.

A critical need by government agencies for more efficient methods of creation, storage, and retrieval of public records has led to the adoption of varied software and information technology systems for creating, managing, and storing records in a digital format. While the advantages of such systems are many, the complexity of safeguarding the integrity of records has increased, requiring greater attention to issues relating to security, accuracy, reliability, and accountability.

These guidelines provide all levels of government within North Carolina direction in establishing methods and procedures for creating or maintaining trustworthy records produced by information technology systems. This guide addresses paper records that are scanned, or imaged, into a digital format, as well as records created in electronic format. Implementation of these guidelines should increase the reliability and accuracy of records regardless of the type of storage media employed, thereby enhancing their admissibility and acceptance by the courts as being trustworthy. Compliance with these guidelines can be demonstrated by the maintenance of an Electronic Records Policy and Self-Warranty form (see Appendix B for a model policy).

These guidelines do not address all emerging electronic records management issues. This document should not be considered authoritative regarding issues such as digital alteration; digital rights management; privacy, security, and encryption; or intellectual property considerations.

The North Carolina guidelines are based on those contained in the Association for Information and Image Management (AIIM) technical report series, Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Systems (AIIM Catalog No. TR31). The technical reports may be purchased from AIIM.

Association for Information and Image Management
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910

Tel: 301/587-8202Fax: 301/587-2711

Website: www.aiim.org

2 Definitions

- Authenticity
- Certified Copy
- Duplicate Record
- Electronic Record
- Electronically Stored Information
- Imaging
- Information Technology System
- Original Record
- Permanent Record
- Preservation Duplicate Record
- Process or System
- Public Record
- Record

- **Authenticity**: The quality of being genuine, not a counterfeit, and free from tampering. Authenticity is typically inferred from internal and external evidence, including its physical characteristics, structure, content, and context. Authenticity is closely associated with the creator (or creators) of a record. First and foremost, an authentic record must have been created by the individual represented as the creator. Federal rules of evidence stipulate that to be presumed authentic, records and documents must be created in the 'regular practice' of business and there must be no overt reason to suspect the trustworthiness of the record. An authentic copy is one that has been officially certified, especially so that it may be admitted into evidence.[1]

- **Certified Copy**: Certified copies have the force of original records. Any public official who causes a record to be copied must attest to it and certify on oath that it is an accurate copy of the original.

- **Duplicate Record**: A record that is produced by the same impression as the original, or from the same matrix, or by any other technique that accurately reproduces the original. Duplicate records accurately reproduce original records, except that duplicates may contain production,

[1] Authentic, *A Glossary of Archival and Records Terminology*, www2.archivists.org/glossary/terms/, accessed November 2012.

control, indexing, certification, or other data not related to informational content of the records and that do not affect the content of the records. When duplication processes change informational content of the records, the resulting records are considered to be new originals. According to the North Carolina Evidence Code, "a duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."[2]

- **Electronic Record**: A record created or reproduced in any medium by means of any system requiring the aid of electronic technology to make the record intelligible by a person, and which is dependent upon a combination of hardware, software, and computer files. "Electronic record" refers to both records created electronically and digitization of records created in other formats. Electronic records must meet the same legal requirements as paper records. Under G.S. § 66-317, ("Enacted Statutes G.S. § 66-317" 2000), a record may not be "denied legal effect or enforceability solely because it is in electronic form." Additionally, "if a law requires a record to be in writing, an electronic record satisfies the law provided it complies with the provisions of this Article."[3] This definition does not include microform records, which can be read with the aid of a magnifying glass.[4]

- **Electronically Stored Information**: Information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software.[5]

- **Imaging**: The process of copying documents by reproducing their appearance through photography, micrographics, or scanning. Imaging, by itself, makes no attempt to make any text in the document machine-readable, although a system may use optical character recognition to convert imaged text to such form. Imaging, especially scanning, is often used to copy paper documents into a document management system that provides the ability to access the images.[6]

---

[2] N.C.G.S. §8C Rule 1003. Evidence Code.
[3] N.C.G.S. §66-317(12). Uniform Electronic Transactions Act. (2000).
[4] Electronic Record, *A Glossary of Archival and Records Terminology*, www2.archivists.org/glossary/terms/, accessed November 2012.
[5] Withers, Kenneth. "Electronically Stored Information: the December 2006 Amendments to the Federal Rules of Civil Procedure." *Sedona Conference Journal.* 7 (Fall 2006): 1.
[6] "Imaging," *A Glossary of Archival and Records Terminology,* www2.archivists.org/glossary/terms, accessed March 2013.

- **Information Technology System**: Any process or system that employs a photo-optical, magnetic, electronic, or other digital device for producing, reproducing, sending, receiving, storing, displaying, or processing records.[7]

- **Original Record**: A record prepared in the first instance or any counterpart intended to have the same effect by a person executing or issuing it. If data is stored in a computer or similar device, any printout or other output readable by sight shown to reflect the data accurately is an 'original.' Original records may present information in a form different from the original information without affecting its quality. For example, information preserved in digital format may be printed on paper using different fonts at different times. When a file is copied to the same or to a different device, it is still considered an original record presuming the copy was successful. Accurate reproductions of the record for the purpose of greater durability, without any added information, are considered preservation duplicates as described below.

- **Permanent Record**: Material created or received in the conduct of affairs and intended to be preserved indefinitely because of the enduring value of the information contained in the record or as evidence of the functions and responsibilities of the record's creator. The ongoing usefulness or significance of records is based on the administrative, legal, fiscal, evidential, or historical information they contain.[8]

- **Preservation Duplicate Record**: A copy of the original that is durable, accurate, complete, and clear, copied in media with greater durability than the original, such as microfilm. Copies have the same force and effect for all purposes as the original record whether the original record is in existence or not. A transcript, exemplification, or certified copy of a preservation duplicate is deemed for all purposes to be a transcript, exemplification, or certified copy of the original record.

- **Process or System**: Any information technology system.

- **Public Record**: "All documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received

---

[7] Adapted from "information processing system" definition. N.C.G.S. §66-312(12). Uniform Electronic Transactions Act. (2000).
[8] Permanent Record, *A Glossary of Archival and Records Terminology*, www2.archivists.org/glossary/terms/, accessed November 2012.

pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions. Agency of North Carolina government or its subdivisions shall mean and include every public office, public officer or official (state or local, elected or appointed), institution, board, commission, bureau, council, department, authority or other unit of government of the state or of any county, unit, special district or other political subdivision of government."[9]

- **Record**: Information or data in any medium that may be used as evidence or proof, and which is created by, received by, sanctioned by, or proceeding from an individual acting within his or her designated capacity. An official record, as distinguished from drafts, convenience files, or personal papers, is the complete, final and authorized copy of a record, and may warrant further actions to ensure its preservation over time.[10]

3 Applicability of Guidelines and Self-Warranty

These guidelines are designed to be applicable to public records produced by any information technology system regardless of the physical characteristics of the record media or technology employed. These guidelines are not intended to replace or exempt government entities from their responsibilities surrounding access to or confidentiality of records under G.S. § 132, nor do they supersede current records retention and disposition schedules. Failure to comply with public records law and retention schedules may result in fines or other penalties.

For state agencies. Records produced by state agencies must be retained for the period of time required by agency records retention and disposition schedules or the General Schedule for State Agency Records. If a state agency maintains any of its permanent records or records with a retention period of at least ten years in an electronic format, the agency is required to fill out an Electronic Records Policy and Self-Warranty form to ensure the authenticity and accuracy of the electronic records produced by the agency (see Appendix B).

- Agency records retention schedules are available here: **www.stateschedules.ncdcr.gov/**

[9] N.C.G.S. § 132-1(a). Public Records.
[10] Adapted from "record" definition, *A Glossary of Archival and Records Terminology*, **www2.archivists.org/glossary/terms/**, accessed November 2012.

- The General Schedule for State Agency Records are available here: www.ncdcr.gov/Portals/26/PDF/schedules/GeneralSchedule_StateAgencies.pdf

To ensure that an agency's Records Retention and Disposition Schedules are accurate and current, contact the Government Records Section, Division of Archives and Records.

For local agencies. Records produced by local agencies must be retained for the period of time required by local records retention and disposition schedules. Contact the Government Records Section if any of the agency's permanent records are stored electronically, as certain permanent records maintained in electronic form must also exist as a paper or microfilm preservation duplicate copy in compliance with the Department of Cultural Resources' *Public Records Requiring Human-Readable Preservation Duplicates* policy. When a local agency converts a paper record group to a digital format, the agency is required to complete an Electronic Records Policy and Self-Warranty form to guarantee the authenticity and accuracy of the electronic records produced by the agency. In order to destroy non-permanent paper records after conversion to a digital format, the local agency is required to submit Section 8, the *Request for Disposal of Original Records Duplicated by Electronic Means* form, of the Electronic Records Policy to the Government Records Section (see Appendix B).

- County and municipal records retention and disposition schedules are available on the State Archives website (www.ncdcr.gov/archives) under the "For Government" tab.
- The *Public Records Requiring Human-Readable Preservation Duplicates* guidance is available on the State Archives website (www.ncdcr.gov/archives) under the "For Government" tab.

For the purpose of security back-up, the State Archives of North Carolina provides assistance with the conversion of permanent records from digital to analog format. Contact the records management analyst in charge of microfilming for further instruction.

Other resources. Government officials may also find the following resources useful:

- David Lawrence's Public Records Law for North Carolina Local Governments provides a comprehensive guide to the state's public records laws and their interpretation by the courts.
- The Department of Cultural Resources' publication Management and Preservation of Digital Media provides further guidance about the maintenance of electronic information over time.

This guidance is available here:
www.ncdcr.gov/Portals/26/PDF/guidelines/AH_Best_Practices_Digital_Preservation.pdf

4 Use of Records Prepared by Information Technology Systems in Legal Proceedings

- Rules of Evidence
- Laying a Proper Foundation
- Life Expectancy of Media and Admissibility of Records
- Legal Status of Records Offered as Evidence
- Admissibility of Records Transferred or Converted to Another Medium

Rules of Evidence. Modern rules of evidence are based on statutes and special rules determined by the courts. The federal government follows the Federal Rules of Evidence, which specifically include documents set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation, or duplicates of such when allowed by law. The federal government is also governed by the Federal Rules of Civil Procedure, which permits parties to request electronically stored information stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form. The North Carolina Rules of Evidence, (G.S. § 8C-1, Article 10, Rule 1001), the North Carolina Rules of Civil Procedure (G.S. § 1A), and the Uniform Electronic Transactions Act (G.S. § 66-311) establish the admissibility of records in evidence in North Carolina courts. The language used in these state statutes follows that of the Federal Rules of Evidence. Documents set down by mechanical or electronic recording are admissible as evidence, as are duplicates of such when allowed by law.

Laying a Proper Foundation. Laying a foundation is "the practice or requirement of introducing evidence of things necessary to make further evidence relevant, material or competent." Courts have determined what is required in laying a proper foundation for electronic records: a witness must show (1) the input procedures used, (2) the tests for accuracy and reliability, and (3) that an established business relies on the computerized records in the ordinary course of carrying on its activities. [11]

[11] *United States v. Russo*, 480 F.2d 1228 (6th Cir.1973)

Rules of evidence permit original and duplicate records to be admitted into evidence provided that a proper foundation is laid by a showing that the records are authentic. According to the Federal Rules of Evidence and corresponding rules in the North Carolina General Statutes, a duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original. As an example, computer printouts are considered original records if an appropriate witness convinces the court that the printouts accurately reflect the information in the electronic files. To guard against questions of authenticity, duplicate records can be authenticated as identical to the original by hash validation.

Federal Rules of Civil Procedure state that a party should produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request. Unless a requesting party specifies the format in which electronic documents should be produced, electronically stored information should be produced in the format in which it is maintained, or in a format that is reasonably useable.

New information system technologies are subject to greater scrutiny in court when determining admissibility. The complex nature of computer storage calls for a more comprehensive foundation. Common assaults on the integrity of information systems include challenges to:

- The source of the input data and the process for transcribing it to machine-readable form
- The process that creates, edits, and updates the files
- The process that produces the output or retrieves the records
- The reliability of the equipment and vendor-supplied software
- The modifications and/or copying of the original files used in preparing data for discovery or evidence production, and the production of copied files, not the originals

When laying a proper foundation for electronic records submitted as evidence, up-to-date documentation that describes the procedural controls employed in creating records must be produced. The original source of the computer program must be delineated, and procedures for input control including tests used to assure accuracy and reliability must be presented.[12] Care must be taken when selecting a witness competent to testify, although the preparer of a record is not required to establish

[12] *Rosenburg, v. Collins*, 624 F.2d 659, 665 (5th Cir. 1980)

an electronic record's authenticity. Furthermore, special care must be exercised by investigators or prosecutors in preserving the chain of custody of the evidence. The existence of an electronic records policy (see Appendix B) and regular system and administrative audits of the process may contribute to the proper foundation needed for admissible electronic records.

Legal Status of Records Offered as Evidence. The structural integrity of records stored in information technology systems is determined independently from the authenticity or factual validity of the record's content based on the accuracy of the process that produced it. When determining the admissibility of records into evidence, the court will consider the reliability and accuracy of the process or system used to produce or reproduce the records. The particular form or format of the records shall have no bearing on their legal status regarding admissibility. Likewise, the destruction of original records after imaging shall not affect the legal status of duplicate records regarding their admissibility.

All that is required for electronic records to be deemed admissible is a prima facie showing that the process or system is trustworthy in terms of producing an accurate result. Once the records are admitted, the trustworthiness of their content will remain subject to challenge. For example, a computer printout of a record is admissible if it is shown to be an accurate reflection of the source data used to create the record, but this does not mean the source data is necessarily correct.

Admissibility of Records Transferred or Converted to Another Medium. The life expectancy of the storage media has no bearing on the admissibility of the records maintained on the media. The transfer or conversion of records from one medium or technology to another should not affect the records' admissibility as evidence provided that quality and accuracy do not functionally change. Electronically stored records need to be actively managed and audited in order to ensure that the information does not change, become corrupted, or become less accessible. As electronic storage media deteriorates, it is necessary to periodically migrate, convert, regenerate, copy, or transfer the records from one medium or format to another in order to preserve the records and make them accessible. An agency should inspect its media and plan to migrate documents to a new medium as necessary, generally every three to five years. For example, if an agency stores its records on CDs or DVDs, these media should be audited annually and records should be copied onto new DVDs after three years. All corresponding information should be properly maintained and carried forward.

Metadata is important ancillary information that must be generated and maintained in order to prove that the records remain the same following conversion or migration. Such ancillary information may include:

- Hashing records to create a unique identifier or digital fingerprint. Those results become part of the record and should be maintained alongside the original record.
- Periodically confirming the original hash by re-running the algorithm tool to ensure that the hash/fingerprint has not changed.
- Maintaining a log of activities on the record, including audit information and access records.

For more information about secure data transfer, consult the State Archives Digital Records Policies and Guidelines page the State Archives website (www.ncdcr.gov/archives) under the "For Government" tab.

5 Availability for Outside Inspection for Purpose of E-discovery

The information system and records produced by it must be made available for pretrial discovery in order to facilitate effective cross-examination.

- Availability of Process or System
- Availability of Records

Availability of Process or System. The process or system used to produce or reproduce records introduced into evidence is subject to outside inspection by opposing parties, the court, and government representatives. Outside inspection may involve:

- Review of procedures documentation
- Review of system operation
- Independent inspection and quality control tests
- Independent audit
- Testing of process or system operation
- Review of equipment design and software documentation
- Review of training programs
- Any other matter related to the operation of the process or system
- Review of documents related to outsourcing including the contract and service level agreements, as well as any quality control procedures followed when documents are returned.

If the records were produced on the current system or a substantially similar system, access to the system may be required to be provided to outside parties upon request so that they may process their own test data.

Availability of Records. Records must be available for inspection and audit by a government representative for the full period required by law and approved records retention schedules, regardless of the life expectancy of the media. Records must continue to exist when litigation, government investigation, or audit is pending, imminent, or, in some cases, foreseeable. In some instances, a court order may prohibit specified records from being destroyed or otherwise rendered unavailable. Records classified as "permanent" on a records retention schedule must be accessible indefinitely because of their enduring value.

System failures, errors in conversion, technical obsolescence, accidental erasure, and inability to read records do not relieve an organization of its obligation to retain and preserve records. Unexpected problems resulting from natural causes may mitigate the level of penalties, but do not relieve an agency of its responsibility to maintain records. Retrieval of permanent records after a natural disaster will be required regardless of cost. See Section 10 of this document, Other Considerations, for more information about disaster backup and restoration.

Records custodians should create and save records in a method that will allow the records to be accessible in the future. Proper file naming and file formats are critical components of enabling access to the files in the future. Notably, the date should be included in the file name, as "date modified" and "date created" metadata tags can sometimes change if electronic information is moved from one storage medium to another. The following DCR guidelines can assist with these aspects of electronic records management.

- *Archival Process for Data and Image Preservation: The Management and Preservation of Digital Media:* **www.ncdcr.gov/Portals/26/PDF/guidelines/AH_Best_Practices_Digital_Preservation.pdf**
- *File Format Guidelines for the Management and Long-term Retention of Electronic Records:* **www.ncdcr.gov/Portals/26/PDF/guidelines/file_formats_in-house_preservation.pdf**
- *Best Practices for File Naming:* **www.ncdcr.gov/Portals/26/PDF/guidelines/filenaming.pdf**

6 Characteristics of Trustworthy Electronic Records

The following are criteria for assessing admissibility of records into evidence. The records must:

- Provide the substance and detail required by law or regulation
- Be legible, accurate, and complete in that all features essential to an accurate reading or comprehension of the record are present
- Be sufficiently complete to fulfill the intent of the applicable law or regulation and the need for that information as stated in the law or regulation
- Attain a sufficient level of accuracy to ensure the utility of the information for the intended legal purpose
- Be accessible and be provided in a standard form of communication within the statutorily required time, if provided, or within a reasonable time, following any request for records and information
- Be retained for the period of time required by municipal, county, or state agency records retention schedules or the General Schedule for State Agency Records.

The presence of the following characteristics of electronic records demonstrates that the process or system is reliable and accurate, and will be more readily admissible as evidence. Records should be:

- Created or recreated as part of a regularly conducted activity
- Created by methods that ensure accuracy
- Created in a timely manner
- Separated into confidential and non-confidential information
- Associated and linked with appropriate metadata

Produced or reproduced as part of a regularly conducted activity. Records produced or reproduced in the regular course of business are admissible if it can be established that the process or system used to produce them is reliable and accurate. A regularly conducted activity may include a regular pattern of activity to produce the records on a daily, weekly, monthly, yearly, or other cyclical schedule. A regularly conducted activity may also include records created as part of a regular program of the organization, but at irregular times. For example, when a planned program results in the one-time reproduction of records created, this is considered a program proceeding in the regular course of business, even though the reproduction only occurred once. This occurs when an agency does a “backfile” conversion of its records, as when paper records are scanned into an electronic or digital imaging system. The record then exists in paper and digital form and both serve as records. Typically,

an office would only do a backfile conversion one time. Once the records are in the system, they would not be scanned again.

Produced by methods that ensure accuracy. The process or system used to generate records may include systematic quality control and audit procedures, as well as operational oversight by someone with detailed knowledge of the process or system. If an agency uses an information technology system to create, manage, and store its records, the agency must have established written policies and procedures that describe how a record is created, named, saved, accessed, audited, and transferred from one storage medium to another. All documentation about the system, and any audit testing or log, needs to be maintained by the agency in order to ensure its accuracy.

Produced in a timely manner. Records produced within a short period after an event or activity occurs tend to be more readily acceptable as accurate than records produced long after the event or activity. However, a challenge to the admissibility of a record produced long after the event can be overcome by a showing that the time lapse had no effect on the record's contents. For example, a statistical report produced annually in the regular course of business can be shown to accurately consolidate data compiled over the course of a year.

Separated by confidential and non-confidential information. The information technology system should be able to separate confidential from non-confidential information. A system's inability to carry out this function cannot be used to deny inspection or examination of public records. Because the agency must bear the costs associated with separating such information, it is recommended that the system have this function built in to save time and expense when requests for inspection or copies are filled.

Where records are managed and accessed through a file browser rather than another information technology system, data creators can organize their directories to reflect whether if files within a folder contain confidential information. Simple solutions may be adequate; creating a folder with “confidential” as part of the title gives notice that the folder contains files with confidential information. Internally, sensitive information can also be maintained by administering appropriate read/write access controls to files or folders and by storing such information in specific locations on off-network storage systems.

Associated and linked with appropriate metadata. Electronic records may contain metadata, or additional data about the content of an electronic record that may not be immediately visible. Metadata can show:

- Means of creation of the data
- Purpose of the data
- Time and date of creation
- Creator or author of data
- Placement of data on a computer network
- File type
- Standards used
- Hashing records
- Other hidden data

According to the North Carolina Rules of Civil Procedure, "electronically stored information" includes all "reasonably accessible metadata that will enable the discovering party to have the ability to access such information as the date sent, date received, author, and recipients. The phrase does not include other metadata unless parties agree otherwise or the court orders upon motion of a party and a showing of good cause for the production of certain metadata." Employees should maintain essential metadata as part of the public record. Examples of such metadata may include:

- E-mail header information which details the path a message takes. This metadata is usually hidden from a user's view and does not appear when e-mail is printed.
- File creator name
- Date created
- Title (stored as the file name)
- Log of activity on the records, including an audit of who has access to the records, when and how often records were accessed, and what information changed
- Cell formulae for spreadsheets

Metadata does not typically print and is sometimes "hidden," which introduces challenges in terms of management and production. This means that employees should not necessarily consider printing and

interfiling documents as a retention technique, as printing and interfiling is done at the expense of lost metadata.

These recommendations are not meant to direct public employees to create information or public records they would not normally create. Creating and maintaining all metadata is not feasible, useful, or advised. Employees should commit to maintaining only the metadata that is essential for a file's current use and/or retention.

For guidance concerning the maintenance of essential metadata connected with a public record, see Metadata as a Public Record in North Carolina: Best Practices Guidelines for Its Retention and Disposition here: **www.ncdcr.gov/Portals/26/PDF/guidelines/Metadata_Guidelines.pdf**

7 Components of the Process or System Used to Prepare Records

A review of the components of a process or system may determine how well the preparation of records is controlled. The admissibility of records can be successfully defended from challenge to the trustworthiness of the process if the process or system includes the following components:

- Procedures
- Training Programs
- Audit Trails
- Audits

Procedures. The trustworthiness of an agency's records offered in evidence may be judged by its established procedures and how closely those procedures are followed. Procedures should provide for consistent quality control and demonstrate what the organization plans to do in managing and controlling the process or system. Deviations from established procedures will be closely scrutinized, especially if the deviations are from legally required procedures.

Examples of system procedures that the agency should maintain include:

- An electronic records and imaging policy. This should document how electronic records are managed in-office. This policy should be applied consistently when records are created, copied, modified, or duplicated. See Appendix B for a model electronic records policy.

- Procedures for security backup files, which should be a part of a larger continuity of operations plan. These procedures should comply with the Department of Cultural Resources' publication,

Security Backup Files as Public Records in North Carolina: Guidelines for the Recycling, Destruction, Erasure, and Re-use of Security Backup Files, available here: www.ncdcr.gov/Portals/26/PDF/guidelines/BackupsProceeds.pdf

- Procedural manuals describing in detail the proper use of information technology systems used by the agency, such as imaging software and hardware or content management systems.

Training Programs. Formal training programs about system procedures create basic presumption in court that the procedures were correctly followed. If an organization can show the court that staff knew what procedures they were supposed to follow, it can also show that there is a high likelihood that the procedures were in fact followed. All employees, including information technology staff responsible for system maintenance, should be made aware of these policies, be trained on them, and should confirm by initialization or signature that they are aware of the policies and have received training on them.

Training documentation should include documentation of distribution of the written procedures, course materials, attendance of individuals at training sessions, remedial or refresher training programs, certifications of training completion, dates, and other relevant information.

Audit Trails. Audit trails document what activities took place as part of the process or system. Audit trails document the identity of the individual(s) who creates, duplicates, modifies, or otherwise prepares the records, what actions are taken by the individual during the course of the process, and when these actions are taken, and describe the results. Properly implemented, audit trails can demonstrate who accessed the system, whether staff followed standard procedures or whether fraud or other unauthorized acts occurred or might be suspected. They can also provide independent confirmation that proper procedures were followed.

Audits. Audits performed periodically on the information technology system confirm that the process or system produces accurate results and confirm that the processes actually used follow the procedures set forth in the documentation. Audits should be designed to evaluate the process or system's accuracy, timeliness, adequacy of procedures, training provided, and the existence of audit trails. No particular method of auditing is required for a record, whether original or duplicate, to be admitted as evidence. Audits can take a number of forms:

- Quality control performed by individuals creating the records to verify the accuracy of records at the time of creation. Quality control is used to ensure the accuracy of the system for operational purposes.
- System audits to confirm that systems are appropriate and efficient.
- Administrative audits to detect compliance with regulations and assess risk of fraud.

Audits confirm the accuracy of the process or system for purposes of admissibility of records in evidence. When ruling on the admissibility of the records, courts may require that audits be performed by an independent source (i.e., persons other than those who created the records or persons without an interest in the content of the records, such as a trained auditor who has organization-wide audit responsibilities).

State agencies should adhere to the General Schedule for State Agency Records regarding audits of, and audit trails for, electronic information. The audit trail file containing data generated during the creation of a master file or database should be maintained in office until its administrative value ends.

8 Documentation of the Process or System

Documentation provides enduring verification of the process or system used to create or recreate records. Recorded documentation preserves the information about the process or system independently from the individuals involved and can be used to prepare exhibits to guide witness testimony. Generally speaking, this documentation can be introduced into evidence for the jury to scrutinize during their deliberations. The following elements should be considered when producing system documentation:

- Content of System Documentation
- Retention of System Documentation

Content of System Documentation. In some proceedings, a general, non-technical description of the process or system will be sufficient. In others, more detailed documentation may be required by the courts, including audit history that verifies that any equipment or software involved was operating properly at the time the records were produced. Documentation should be reviewed and updated on a regular basis.

For purposes of laying a foundation for admissibility of records into evidence, actual system procedures followed during the period that the records in question were produced should be maintained in sufficient detail to enable a qualified witness (e.g., the records custodian) to rely on the

documentation in describing the process or system to the court. The documentation should explain what should have been done and what was actually done, and explain any deviations from standard procedures. The training, audit trail, and audit documentation should also be presented to confirm the accuracy of the process or system.

Retention of System Documentation. At least one set of documentation should be maintained during the period for which the records produced by the process or system could likely be subject to court review. When the documentation changes, old versions should continue to be maintained for the same period of time the records themselves need to be kept per the records retention and disposition schedules. The court will determine the admissibility of the records into evidence based on the accuracy of the process or system in effect at the time the records were produced.

9 Special Considerations for Digital Imaging

Imaging, or scanning, is the process of converting human readable media, such as paper or microfilm, into information that can be stored and retrieved electronically. Implementing a digital imaging system may allow for easier capture, storage, retrieval, and sharing of data, provided proper metadata and indexing exists for imaged records. The following components must be considered when implementing an imaging system:

- Documentation
- Indexing and Other Metadata
- Records Quality
- Auditing
- Records Retention
- Considerations when Choosing a System

Documentation. Documentation should describe the process or system used to produce and manage the agency's imaged records. Documentation should be complete and up-to-date. Documentation, in conjunction with training, increases the likelihood that staff is aware of and follows the most current procedures. It also ensures that reliable system documentation is immediately available if needed for court proceedings.

Documentation about the imaging system and process should establish the steps required to get from the beginning to the end of the process. It should describe the system hardware and software, the system environment in terms of the organizational structure, functions and responsibilities, and the

system processes. Documentation should also include a description of the records produced and the processes of records disposition, as well as:

- The resolution of scanned images
- The file formats of scanned images
- The file naming conventions used for scanned images
- Whether batch conversion or file re-naming will be necessary, and what tools are used for such conversions

Indexing and Other Metadata. To assure that the imaged documents remain accessible, an indexing database that facilitates efficient retrieval, ease of use, and up-to-date information about the digitized records stored in the system should be developed. This index should capture the content, structure, and context of the imaged records. Additionally, whatever media is used to store imaged data should be clearly labeled with enough information that the contents of the storage medium can be determined.

Records Quality. The following features of a digitized record should be legible with sufficient clarity after imaging so that each can be recognized:

- Individual letters, numbers, and symbols
- Combinations of letters, numbers, and symbols forming words or sentences
- Graphics such as signatures, logos, and pictures
- Other features of records such as color, shape, texture, etc., that relate to the content of the information

Imaging and image enhancement techniques (i.e., techniques for processing the image so that the result is visually clearer than the original image) may be used provided that they do not change the content of the records. If image enhancement techniques are used, the information that is readable or recognizable on duplicates should also be readable or recognizable on originals. It may be advisable to document how such enhancements are made in the imaging process documentation. If image enhancement is performed, an original un-altered copy of the image should be stored in addition to the altered image.

Auditing. Audits should be performed routinely on imaged records to ensure no information has been lost during the imaging process, and audits should be adequately documented. For duplicates, audits also should confirm that the duplicates accurately reproduce the originals. This normally involves

comparing statistically valid samplings of originals to their corresponding reproductions prior to any destruction of the originals. The actual audit reports indicate whether the statistically valid sampling of records produced accurate results and what remedial procedures were followed if the expected level of accuracy was not achieved.

Records Retention. Creating digital copies of records does not remove the original records from the records retention schedule. If a state agency is considering imaging its files, contact the agency's records analyst to amend its records retention schedule to allow for the destruction of the original paper copy. If a local agency is considering imaging its files, it must request and record approval for the destruction of the original paper records for each new records series to be scanned through the "Request for Disposal of Original Records Duplicated by Electronic Means" form. This form is located within the Electronic Records Policy (see Appendix B) and must be approved by the agency's records analyst before any originals may be destroyed.

Considerations when Choosing an Imaging System. A state agency may use either the scanning service provided by the North Carolina Office of Information Technology Services, or scan in-house. North Carolina Office of Information Technology Services scanning services can be found here: **www.itstaff.state.nc.us/ConvenienceContracts/SuppStaff/Categories.asp?ID=29**

A local agency may scan in-house or outsource its imaging services. It may choose from those vendors available to state agencies, but is not bound to those vendors.

If the agency scans in-house, it should have a training component and employees are required to sign off that they received the training. If an agency outsources its scanning, it should maintain a copy of the purchase order and a detailed service-level agreement (see Section 10 of this document, Other Considerations, for more about contracting).

Additional Guidance.

- The Department of Cultural Resources' publication Digital Imaging Systems Guidelines is available here: **www.ncdcr.gov/archives/ForGovernment/DigitalRecords/DigitalRecordsPoliciesandGuidelines.aspx#imaging**
- An electronic records policy template, a component of which is the model imaging policy, is located in Appendix B of this document.

10 Other Considerations

- System Planning
- Records Management
- Database Indexing
- Security and Disaster Backup and Restoration
- Cloud Computing
- Contracting

System planning. A thorough examination of an agency's entire record keeping system should precede the purchase of any system. System documentation, system access records, digitization and scanning records, metadata, and information maintained by that system must be listed in an approved records retention and disposition schedule prior to their destruction or other disposition. The Government Records Section is able to assist agencies with this process, and with the review of planning documentation previously mentioned.

When planning system use, records retention should be considered before implementation. Records or information with relatively short retention requirements may be best suited for storage in traditional paper media or electronic systems. Microfilm may be used as an alternative to computer readable media if long-term or permanent retention is necessary. Its stability, ease of duplication, and immunity from obsolescence make it more suitable as a preservation duplicate medium. If an agency is interested in microfilming, it should consult the agency's records analyst, as the agency's retention schedule may need to be amended. The Collections Services Section of the State Archives of North Carolina provides microfilming services for certain records series produced by agencies.

Following the identification of retention requirements, if the agency determines that the proposed information technology system is the best storage methodology, the agency should make provisions for routine upgrades. Upgrades or migrations to new hardware and software, particularly on an enterprise-wide scale, can be expensive, so future budgetary implications should be considered prior to purchasing an information technology system. Because it is difficult at best to predict those costs, a certain percentage of the startup cost should be built into initial budgets for the purpose of future conversions. Before entering into a purchase contract, agencies should determine from the vendor the cost of extracting data from the system should they need to do so. This cost may be built into the contract, or it may be an additional fee or service.

A change request must be filed by state agencies with the Office of Information Technology Services when total cost of ownership for IT projects exceeds $500,000.

Records Management. Other records management factors that are commonly thought to apply only to paper-based systems should be addressed. These include security, access to and examination of data, duplication procedures to meet public records requests, and rendition and revision control of inactive or archived records. Other considerations, such as identifying and cataloging metadata, are unique to information technology systems.

Electronic records are subject to records retention schedules according to their content, not their format. Schedules also provide information explaining which files should be kept in case of audit, computer usage, security incidents, and the proper storage and deletion of electronic information.

Unless otherwise specified, in case of court order or public records request, records should be produced in the order in which they were created or maintained in the order of business.

Database Indexing. G.S. §132-6.1 requires that electronic databases that meet certain criteria be indexed. These indexes can be relatively simple or complex depending on the type of data indexed and how the database is used. The Government Records Section provides guidance on indexing databases, available here: **www.records.ncdcr.gov/erecords/pubdata/default.htm**

Security and Disaster Backup and Restoration. Security backups are critical to the survival of electronic data. Human or natural disasters, accidents involving the handling of media, and human error make electronic media vulnerable to damage. According to state policy, security backup files are public records [according to G.S. § 121-2(8) and § 132-1] and may not be disposed of, erased, or destroyed (according to G.S. § 132-3) without specific guidance from the Department of Cultural Resources. Backup policies should be a component of a continuity of operations plan, and should comply with the following policies:

- Security Backup files as Public Records in North Carolina: Guidelines for the Recycling, Destruction, Erasure, and Re-use of Security Backup Files available at **www.ncdcr.gov/Portals/26/PDF/guidelines/BackupsProceds.pdf**

- The Statewide Information Security Manual available at www.scio.nc.gov/library/pdf/StatewideInformationSecurityManual/Security_Manual_update_June_30_2011.pdf

Cloud Computing. State and local governments may elect to use cloud-based technologies for the creation and storage of some electronic information. For more information, consult the Best Practices for Cloud Computing: Records Management Considerations, located here: www.ncdcr.gov/archives/ForGovernment/DigitalRecords/DigitalRecordsPoliciesandGuidelines.aspx#cloud

Contracting. If a government entity contracts with a third party to image records or for other records management services, the terms of the service level agreement should detail how the contractor provides security, confidentiality, storage, and back-ups for electronic records. It should describe the storage environment, including any geographically disparate storage locations, and how the contractor complies with records retention laws, including what the contractor is able to reproduce should legal proceedings or public records requests be issued. The contract should also describe how the contractor avoids spoliation of evidence once e-discovery has commenced.

Appendix A: Excerpts of Relevant North Carolina General Statutes

- Chapter 121: Archives and History
- Chapter 132: Public Records
- Chapter 66, Article 11A: Electronic Commerce in Government
- Chapter 66, Article 40: Uniform Electronic Transactions Act
- Chapter 8, Article 3: Public Records
- Chapter 8, Article 4A: Photographic Copies of Business and Public Records
- Chapter 153A-436: Photographic Reproduction of County Records
- Chapter 160A-490: Photographic Reproduction of Records
- Chapter 47-1A: Rules of Civil Procedure
- Chapter 8C: Evidence Code

Chapter 121: Archives and History

- G.S. § 121-4 Powers and duties of the Department of Cultural Resources.
- G.S. § 121-5 Public records and archives.

G.S. § 121-4 Powers and duties of the Department of Cultural Resources.

(2) To conduct a records management program, including the operation of a records center or centers and a centralized microfilming program, for the benefit of all state agencies, and to give advice and assistance to the public officials and agencies in matters pertaining to the economical and efficient maintenance and preservation of public records.

G.S. § 121-5. Public records and archives.

(a) State Archival Agency Designated. - The Department of Cultural Resources shall be the official archival agency of the State of North Carolina with authority as provided throughout this Chapter and Chapter 132 of the General Statutes of North Carolina in relation to the public records of the State, counties, municipalities, and other subdivisions of government.

(b) (Effective October 1, 1994) Destruction of Records Regulated. - No person may destroy, sell, loan, or otherwise dispose of any public record without the consent of the Department of Cultural Resources. Whoever unlawfully removes a public record from the office where it is usually kept, or alters, mutilates, or destroys it shall be guilty of a Class 3 misdemeanor and upon conviction only fined at the discretion of the court.

Chapter 132: Public Records

11 G.S. § 132-1 "Public records" defined.
12 G.S. § 132-3 (Effective January 1, 1995) Destruction of records regulated.
13 G.S. § 132-6.1 Electronic data processing records
14 G.S. § 132-8.1 Records management program administered by Department of Cultural Resources; establishment of standards, procedures, etc.; surveys.
15 G.S. § 132-8.2 Selection and preservation of records considered essential; making or designation of preservation duplicates; force and effect of duplicates or copies thereof.

G.S. § 132-1. "Public records" defined.

(a) "Public record" or "public records" shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions. Agency of North Carolina government or its subdivisions shall mean and include every public office, public officer or official (State or local, elected or appointed), institution, board, commission, bureau, council, department, authority or other unit of government of the State or of any county, unit, special district or other political subdivision of government.

(b) The public records and public information compiled by the agencies of North Carolina government or its subdivisions are the property of the people. Therefore, it is the policy of this State that the people may obtain copies of their public records and public information free or at minimal cost unless otherwise specifically provided by law. As used herein, 'minimal cost' shall mean the actual cost of reproducing the public record or public information.

G.S. § 132-3. (Effective January 1, 1995) Destruction of records regulated.

(a) Prohibition. - No public official may destroy, sell, loan, or otherwise dispose of any public record, except in accordance with G.S. §121-5 and G.S. § 130A 99, without the consent of the Department of Cultural Resources. Whoever unlawfully removes a public record from the office where it is usually kept, or alters, defaces, mutilates or destroys it shall be guilty of a Class 3 misdemeanor and upon conviction only fined not less than ten dollars ($10.00) nor more than five hundred dollars ($500.00).

§ 132-6.1. Electronic data-processing records.

(a) After June 30, 1996, no public agency shall purchase, lease, create, or otherwise acquire any electronic data-processing system for the storage, manipulation, or retrieval of public records unless it first determines that the system will not impair or impede the agency's ability to permit the public inspection and examination, and to provide electronic copies of such records. Nothing in this subsection shall be construed to require the retention by the public agency of obsolete hardware or software.

(b) Every public agency shall create an index of computer databases compiled or created by a public agency on the following schedule:
State agencies by July 1, 1996;
Municipalities with populations of 10,000 or more, counties with populations of 25,000 or more, as determined by the 1990 U.S. Census, and public hospitals in those counties, by July 1, 1997;
Municipalities with populations of less than 10,000, counties with populations of less than 25,000, as determined by the 1990 U.S. Census, and public hospitals in those counties, by July 1, 1998;
Political subdivisions and their agencies that are not otherwise covered by this schedule, after June 30, 1998.

The index shall be a public record and shall include, at a minimum, the following information with respect to each database listed therein: a list of the data fields; a description of the format or record layout; information as to the frequency with which the database is updated; a list of any data fields to which public access is restricted; a description of each form in which the database can be copied or reproduced using the agency's computer facilities; and a schedule of fees for the production of copies in each available form. Electronic databases compiled or created prior to the date by which the index must be created in accordance with this subsection may be indexed at the public agency's option. The form, content, language, and guidelines for the index and the databases to be indexed shall be developed by the Office of Archives and History in consultation with officials at other public agencies.

(c) Nothing in this section shall require a public agency to create a computer database that the public agency has not otherwise created or is not otherwise required to be created. Nothing in this section requires a public agency to disclose security features of its electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security standards, procedures, processes, configurations, software, and codes.

(d) The following definitions apply in this section:
(1) Computer database. – A structured collection of data or documents residing in a database management program or spreadsheet software.
(2) Computer hardware. – Any tangible machine or device utilized for the electronic storage, manipulation, or retrieval of data.
(3) Computer program. – A series of instructions or statements that permit the storage, manipulation, and retrieval of data within an electronic data-processing system, together with any associated documentation. The term does not include the original data, or any analysis, compilation, or manipulated form of the original data produced by the use of the program or software.
(4) Computer software. – Any set or combination of computer programs. The term does not include the original data, or any analysis, compilation, or manipulated form of the original data produced by the use of the program or software.
(5) Electronic data-processing system. – Computer hardware, computer software, or computer programs or any combination thereof, regardless of kind or origin. (1995, c. 388, s. 3; 2000-71, s. 1; 2002-159, s. 35(i).)

G.S. § 132-8.1. Records management program administered by Department of Cultural Resources; establishment of standards, procedures, etc.; surveys.
A records management program for the application of efficient and economical management methods to the creation, utilization, maintenance, retention, preservation, and disposal of official records shall be administered by the Department of Cultural Resources. It shall be the duty of that Department, in cooperation with and with the approval of the Department of Administration, to establish standards, procedures, and techniques for effective management of public records, to make continuing surveys of paper work operations, and to recommend improvements in current records management practices including the use of space, equipment, and supplies employed in creating, maintaining, and servicing records. It shall be the duty of the head of each State agency and the governing body of each county, municipality and other subdivision of government to cooperate with the Department of Cultural Resources in conducting surveys and to establish and maintain an active, continuing program for the economical and efficient management of the records of said agency, county, municipality, or other subdivision of government.

G.S. § 132-8.2. Selection and preservation of records considered essential; making or designation of preservation duplicates; force and effect of duplicates or copies thereof.
In cooperation with the head of each State agency and the governing body of each county, municipality, and other subdivision of government, the Department of Cultural Resources shall

establish and maintain a program for the selection and preservation of public records considered essential to the operation of government and to the protection of the rights and interests of persons, and, within the limitations of funds available for the purpose, shall make or cause to be made preservation duplicates or designate as preservation duplicates existing copies of such essential public records. Preservation duplicates shall be durable, accurate, complete and clear, and such duplicates made by a photographic, photostatic, microfilm, micro card, miniature photographic, or other process which accurately reproduces and forms a durable medium for so reproducing the original shall have the same force and effect for all purposes as the original record whether the original record is in existence or not. A transcript, exemplification, or certified copy of such preservation duplicate shall be deemed for all purposes to be a transcript, exemplification, or certified copy of the original record. Such preservation duplicates shall be preserved in the place and manner of safekeeping prescribed by the Department of Cultural Resources.

Chapter 66 Article 11A: Electronic Commerce in Government

- § 66 58.3. Certification authority licensing.
- § 66 58.4. Use of electronic signatures.
- § 66 58.5. Validity of electronic signatures.
- § 66 58.9. Exemptions.
- § 66 58.11. Reciprocal agreements.
- § 66 58.12. Agencies may provide access to services through electronic and digital transactions; fees authorized.

§ 66 58.3. Certification authority licensing.

All persons acting as a certification authority with respect to transactions under this Article shall be licensed by the Secretary prior to representing themselves or acting as a certification authority under this Article. Certification authority licensing standards set by the Secretary may include, but are not limited to, technical, physical, procedural, and personnel security controls, repository obligations, and financial responsibility standards. Upon payment of the required fees, a certification authority meeting the standards adopted by the Secretary by rule shall be licensed for a period of one year. Licenses of certification authorities complying with the standards adopted by the Secretary may be renewed for additional one year terms upon payment of the required renewal fee. (1998 127, s. 1.)

§ 66 58.4. Use of electronic signatures.

All public agencies may use and accept electronic signatures pursuant to this Article, pursuant to Article 40 of this Chapter (the Uniform Electronic Transactions Act), or pursuant to other law. (1998 127, s. 1; 2003 233, s. 1; 2007 119, s. 1.)

§ 66 58.5. Validity of electronic signatures.

(a) An electronic signature contained in a transaction undertaken pursuant to this Article between a person and a public agency, or between public agencies, shall have the same force and effect as a manual signature provided all of the following requirements are met:

(1) The public agency involved in the transaction requests or requires the use of electronic signatures.

(2) The electronic signature contained in the transaction embodies all of the following attributes:

a. It is unique to the person using it;

b. It is capable of certification;

c. It is under sole control of the person using it;

d. It is linked to data in such a manner that if the data are changed, the electronic signature is invalidated; and

e. It conforms to rules adopted by the Secretary pursuant to this Article.

(b) A transaction undertaken pursuant to this Article between a person and a public agency, or between public agencies, is not unenforceable, nor is it inadmissible into evidence, on the sole ground that the transaction is evidenced by an electronic record or that it has been signed with an electronic signature.

(c) This Article does not affect the validity of, presumptions relating to, or burdens of proof regarding an electronic signature that is accepted pursuant to Article 40 of this Chapter or other law.(1998 127, s. 1; 2003 233, s. 2.)

§ 66 58.9. Exemptions.

This Article shall not apply to any of the following:

(1) Electronic signatures and facsimile signatures that are otherwise allowed by law.

(2) The execution of documents filed with, issued, or entered by a court of the General Court of Justice. However, a document or transaction validly executed under this Article is not rendered invalid because it is filed with, or attached to, a document issued or entered by a court of the General Court of Justice.

(3) Transactions where a public agency is not a party. (1998 127, s. 1.)

§ 66 58.11. Reciprocal agreements.

The Secretary is hereby authorized to enter into reciprocal arrangements with appropriate and duly authorized public agencies of other jurisdictions having a law substantially similar to this Article so as to further the purpose of this Article. (1998 127, s. 1.)

§ 66 58.12. Agencies may provide access to services through electronic and digital transactions; fees authorized.

(a) Public agencies are encouraged to maximize citizen and business access to their services through the use of electronic and digital transactions. A public agency may determine, through program and transaction analysis, which of its services may be made available to the public through electronic means, including the Internet. The agency shall identify any inhibitors to electronic transactions between the agency and the public, including legal, policy, financial, or privacy concerns and specific inhibitors unique to the agency or type of transaction. An agency shall not provide a transaction through the Internet that is impractical, unreasonable, or not permitted by laws pertaining to privacy or security.

(b) An agency may charge a fee to cover its costs of permitting a person to complete a transaction through the World Wide Web or other means of electronic access. The fee may be applied on a per transaction basis and may be calculated either as a flat fee or a percentage fee, as determined under an agreement between a person and a public agency. The fee may be collected by the agency or by its third party agent.

(c) The fee imposed under subsection (b) of this section must be approved by the Office of State Budget and Management, in consultation with the State Chief Information Officer and the Joint Legislative Commission on Governmental Operations. The revenue derived from the fee must be credited to a nonreverting agency reserve account. The funds in the account may be expended only for e commerce initiatives and projects approved by the State Chief Information Officer, in consultation with the Joint Legislative Oversight Committee on Information Technology. For purposes of this subsection, the term "public agencies" does not include a county, unit, special district, or other political subdivision of government.

(d) This section does not apply to the Judicial Department. (2000 109, s. 8; 2004 129, s. 27; 2005 92, s. 1.)

For more information, see North Carolina Administrative Code Chapter 10: Electronic Commerce Section, available at: www.secretary.state.nc.us/Ecomm/pdf/rules.pdf

Chapter 66, Article 40: Uniform Electronic Transactions Act

- § 66 314. Prospective application.
- § 66 316. Construction and application.
- § 66 317. Legal recognition of electronic records, electronic signatures, and electronic contracts.
- § 66 317. Legal recognition of electronic records, electronic signatures, and electronic contracts.
- § 66 318. Provision of information in writing; presentation of records.
- § 66 321. Notarization and acknowledgment.
- § 66 322. Retention of electronic records; originals.
- § 66 326. Transferable records.

§ 66 314. Prospective application.

This Article applies to any electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after the effective date of this Article. (2000 152, s. 1.)

§ 66 316. Construction and application.

This Article must be construed and applied:

(1) To facilitate electronic transactions consistent with other applicable law;

(2) To be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and

(3) To effectuate its general purpose to make uniform the law with respect to the subject of this act among states enacting it. (2000 152, s. 1.)

§ 66 317. Legal recognition of electronic records, electronic signatures, and electronic contracts.

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law provided it complies with the provisions of this Article.

(d) If a law requires a signature, an electronic signature satisfies the law provided it complies with the provisions of this Article. (2000 152, s. 1.)

§ 66 318. Provision of information in writing; presentation of records.

(a) If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if:

(1) The sender or its information processing system inhibits the ability of the recipient to print or store the electronic record; or

(2) It is not capable of being accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

(b) If a law other than this Article requires a record (i) to be posted or displayed in a certain manner, (ii) to be sent, communicated, or transmitted by a specified method, or (iii) to contain information that is formatted in a certain manner, the following rules apply:

(1) The record must be posted or displayed in the manner specified in the other law.

(2) Except as otherwise provided in subdivision (d)(2) of this section, the record must be sent, communicated, or transmitted by the method specified in the other law.

(3) The record must contain the information formatted in the manner specified in the other law.

(c) If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

(d) The requirements of this section may not be varied by agreement, but:

(1) To the extent a law other than this act requires information to be provided, sent, or delivered in writing, but permits that requirement to be varied by agreement, the requirement under subsection (a) of this section that the information be in the form of an electronic record capable of retention may also be varied by agreement; and

(2) A requirement under a law other than this Article to send, communicate, or transmit a record by regular United States mail may be varied by agreement to the extent permitted by the other law. (2000 152, s. 1; 2001 295, s. 3.)

§ 66 321. Notarization and acknowledgment.

If a law requires a signature or record relating to a transaction to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record. (2000 152, s. 1.)

§ 66 322. Retention of electronic records; originals.

(a) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(1) Accurately reflects the information set forth in the record at the time it was first generated in its final form as an electronic record or otherwise; and

(2) Remains accessible for later reference.

(b) A requirement to retain a record in accordance with subsection (a) of this section does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received.

(c) A person may satisfy subsection (a) of this section by using the services of another person if the requirements of that subsection are satisfied.

(d) If a law requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained in accordance with subsection (a) of this section.

(e) If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection (a) of this section.

(f) A record retained as an electronic record in accordance with subsection (a) of this section satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after the effective date of this Article specifically prohibits the use of an electronic record for the specified purpose.

(g) This section does not preclude a governmental agency of this State from specifying additional requirements for the retention of a record subject to the agency's jurisdiction. (2000 152, s. 1)

§ 66 326. Transferable records.

(a) In this section, "transferable record" means an electronic record that:

(1) Would be a note under Article 3 of Chapter 25 of the General Statutes or a document under Article 7 of Chapter 25 of the General Statutes if the electronic record were in writing; and

(2) The issuer of the electronic record expressly has agreed is a transferable record.

(b) A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

(c) A system satisfies subsection (b) of this section, and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:

(1) A single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in subdivisions (4), (5), and (6) of this subsection, unalterable;

(2) The authoritative copy identifies the person asserting control as:

a. The person to which the transferable record was issued; or

b. If the authoritative copy indicates that the transferable record has been transferred, the person to whom the transferable record was most recently transferred;

(3) The authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(5) Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(6) Any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

(d) Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in G.S. § 25 1 201(21), of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under Chapter 25 of the General Statutes, including, if the applicable statutory requirements under G.S. § 25 3 302(a), 25 7 501, or 25 9 330 are satisfied, the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated, or a purchaser, respectively. Delivery, possession, and endorsement are not required to obtain or exercise any of the rights under this subsection.

(e) Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under Chapter 25 of the General Statutes.

(f) If requested by a person against whom enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record. (2000 152, s. 1; 2000 140, s. 97; 2006 112, s. 24.)

Chapter 8, Article 3: Public Records

- G.S. § 8-34 Copies of official writings
- Case Notes

G.S. § 8-34. Copies of official writings.

(a) Copies of all official bonds, writings, papers, or documents, recorded or filed as records in any court, or public office, or lodged in the office of the Governor, Treasurer, Auditor, Secretary of State, Attorney General, Adjutant General, or the State Department of Cultural Resources, shall be as competent evidence as the originals, when certified by the keeper of such records or writings under the seal of his office when there is such seal, or under his hand when there is no such seal, unless the court shall order the production of the original. Copies of the records of the board of county commissioners shall be evidence when certified by the clerk of the board under his hand and seal of the county.

(b) The provisions of subsection (a) of this section shall apply to records stored on any form of permanent, computer-readable media, such as a CD-ROM, if the medium is not subject to erasure or alteration. Non-erasable, computer-readable storage media shall not be used for preservation duplicates, as defined in G.S. § 132-8.2, or for the preservation of permanently valuable records as provided in G.S. § 121-5(b), except to the extent expressly approved by the Department of Cultural Resources pursuant to standards and conditions established by the Department.

Case Notes

- "Copy" Defined
- Certification of Copy
- Original Record is Admissible

"Copy" Defined. A copy, within the meaning of this section, is a transcript of the original, i.e., a writing exactly like another writing. State v. Champion, 116 N.C. 987, 21 S.E. 700 (1895); Wiggins v. Rogers, 175 N.C. 67, 94 S.E. 685 (1917).

Certification of Copy. The power of an officer, who is the keeper of certain public records, to certify copies is confined to a certification of their contents as they appear by the records themselves, and the records must, therefore, be so certified, for he has no authority to certify to the substance of them, nor that any particular fact, as a date, appears on them. Wiggins v. Rogers, 175 N.C. 67, 94 S.E. 685 (1917).

Original Record Is Admissible. This section does not prevent the admission in evidence of the original record itself. State v. Voight, 90 N.C. 741 (1884); State ex rel. Carolina Iron Co. v. Abernathy, 94 N.C. 545 (1886). See State v. Hunter, 94 N.C. 829 (1886); Charles S. Riley & Co. v. Carter, 165 N.C. 334, 81 S.E. 414 (1914); Blalock v. Whisnant, 216 N.C. 417, 5 S.E.2d 130 (1939).

While certified copies of records are admitted in evidence, the originals are not thereby made incompetent. State v. Joyner, 295 N.C. 55, 243 S.E.2d 367 (1978).

Chapter 8, Article 4A: Photographic Copies of Business and Public Records

- G.S. § 8-45.1 Photographic reproductions admissible; destruction of originals.
- Case Notes

G.S. § 8-45.1. Photographic reproductions admissible; destruction of originals.
(a) If any business, institution, member of a profession or calling, or any department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation, X ray or combination thereof, of any act, transaction, occurrence or event, and in the regular course of business has caused any or all of the same to be recorded, copied or reproduced by any photographic, photostatic, microfilm, microcard, miniature photographic, or other process which accurately reproduces or forms a durable medium for so reproducing the original,

the original may be destroyed in the regular course of business unless held in a custodial or fiduciary capacity or unless its preservation is required by law. Such reproduction, when satisfactorily identified, is as admissible in evidence as the original itself in any judicial or administrative proceeding whether the original is in existence or not and an enlargement or facsimile of such reproduction is likewise admissible in evidence if the original reproduction is in existence and available for inspection under direction of court. The introduction of a reproduced record, enlargement or facsimile, does not preclude admission of the original.

(b) The provisions of subsection (a) of this section shall apply to records stored on any form of permanent, computer-readable media, such as a CD-ROM, if the medium is not subject to erasure or alteration. Nonerasable, computer-readable storage media shall not be used for preservation duplicates, as defined in G.S. § 132-8.2, or for the preservation of permanently valuable records as provided in G.S. § 121-5(b), except to the extent expressly approved by the Department of Cultural Resources pursuant to standards and conditions established by the Department.

Editor's Note: Notwithstanding the above citation, G.S. § 121-5(b) and G.S. § 132-3 (a) require the consent of the Department of Cultural Resources before any public record, original or copy, may be destroyed.

Case Notes

- Admissibility of "Written Hearsay"
- Evidence Reproductions Are Primary
- Photocopies are admissible as originals
- Failure to Show That Copy Was Made in Regular Course of Business or by Whom It was Made

Admissibility of "Written Hearsay". North Carolina countenances the introduction of test results, certified copies of official documents and records, as well as other writings, which, but for statute or decisional authority, would be written hearsay. In re Arthur, 27 N.C. App. 227, 218 S.E.2d 869 (1975), rev'd on other grounds, 291 N.C. 640, 231 S.E.2d 614 (1977).

Evidence Reproductions Are Primary. Reproductions are made and kept among the records of many banks in due course of business. Their accuracy is not questioned. As proof of payment they constitute not secondary but primary evidence. State v. Shumaker, 251 N.C. 678, 111 S.E.2d 878 (1960).

Photostatic copies of deposit slips and checks made by an employee of a bank in the usual course of business and identified by such employee are competent as primary evidence without proof of the loss or destruction of the originals. Jones v. Metropolitan Life Ins. Co., 5 N.C. App. 570, 169 S.E.2d 6 (1969).

Photocopies are admissible as originals. Pinner v. Southern Bell Tel. & Tel. Co., 60 N.C. App. 257, 298 S.E.2d 749, cert. denied, 308 N.C. 387, 302 S.E.2d 253 (1983). Business records are admissible as an exception to the hearsay rule when they (1) are made in the regular course of business, at or near the time of the events recorded; (2) are original entries; (3) are based on the personal knowledge of the individual making the entries; and (4) are authenticated by a witness familiar with the system by which they were made. Pinner v. Southern Bell Tel. & Tel. Co., 60 N.C. App. 257, 298 S.E.2d 749, cert. denied, 308 N.C. 387, 302 S.E.2d 253 (1983).

Failure to Show That Copy Was Made in Regular Course of Business or by Whom It Was Made. A photostatic copy of a purported written designation of plaintiff by deceased as the beneficiary of deceased's governmental life insurance benefits should not be admitted as evidence where plaintiff failed to show that the copy was made in the regular course of business or activity of any federal agency or by whom it was made. Jones v. Metropolitan Life Ins. Co., 5 N.C. App. 570, 169 S.E.2d 6 (1969).

Chapter 153: Photographic Reproductions of County Records

G.S. § 153A-436. Photographic reproduction of county records.

(a) A county may provide for the reproduction, by photocopy, photograph, microphotograph, or any other method of reproduction that gives legible and permanent copies, of instruments, documents, and other papers filed with the register of deeds and of any other county records. The county shall keep each reproduction of an instrument, document, paper, or other record in a fire-resistant file, vault, or similar container. If a duplicate reproduction is made to provide a security copy, the county shall keep the duplicate in a fire-resistant file, vault, or similar container separate from that housing the principal reproduction.

If a county has provided for reproducing records, any custodian of public records of the county may cause to be reproduced any of the records under, or coming under, his custody.

(e) A reproduction, made pursuant to this Article, of an instrument, document, paper, or other record is as admissible in evidence in any judicial or administrative proceeding as the original itself, whether the original is extant or not. An enlargement or other facsimile of the reproduction is also admissible in

evidence if the original reproduction is extant and available for inspection under the direction of the court or administrative agency.
(f) The provisions of subsection (a) of this section shall apply to records stored on any form of permanent, computer-readable media, such as a CD-ROM, if the medium is not subject to erasure or alteration. Non-erasable, computer-readable storage media shall not be used for preservation duplicates, as defined in G.S. § 132-8.2, or for the preservation of permanently valuable records as provided in G.S. § 121-5(b), except to the extent expressly approved by the Department of Cultural Resources pursuant to standards and conditions established by the Department.

Chapter 160: Photographic Reproduction of Records

G.S. § 160A-490. Photographic reproduction of records.
(a) General Statutes 153A-436 shall apply to cities. When a county officer is designated by title in that Article, the designation shall be construed to mean the appropriate city officer, and the city council shall perform powers and duties conferred and imposed on the board of county commissioners.

(b) The provisions of subsection (a) of this section shall apply to records stored on any form of permanent, computer-readable media, such as a CD-ROM, if the medium is not subject to erasure or alteration. Non-erasable, computer-readable storage media shall not be used for preservation duplicates, as defined in G.S. § 132-8.2, or for the preservation of permanently valuable records as provided in G.S. § 121-5(b), except to the extent expressly approved by the Department of Cultural Resources pursuant to standards and conditions established by the Department.

Chapter 1A: Rules of Civil Procedure

- G.S. § 1A-5.Rule 29. Stipulations regarding discovery procedure.
- G.S. § 1A-5. Rule 34. Production of documents, electronically stored information, and things; entry upon land for inspection and other purposes.

G.S. § 1A-5.Rule 29. Stipulations regarding discovery procedure.
Unless the court orders otherwise, the parties may by written stipulation (i) provide that depositions may be taken before any person, at any time or place, upon any notice, and in any manner and when so taken may be used like other depositions, and (ii) modify the procedures provided by these rules for other methods of discovery. (1967, c. 954, s. 1; 1975, c. 762, s. 1.)

G.S. § 1A-5. Rule 34. Production of documents, electronically stored information, and things; entry upon land for inspection and other purposes.

(a) Scope. Any party may serve on any other party a request (i) to produce and permit the party making the request, or someone acting on that party's behalf, to inspect and copy, test, or sample any designated documents, electronically stored information, or tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (ii) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

(b) Procedure. The request may, without leave of court, be served upon the plaintiff after commencement of the action and upon any other party with or after service of the summons and complaint upon that party. The request shall set forth the items to be inspected either by individual item or by category, and describe each item and category with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced.

The party upon whom the request is served shall serve a written response within 30 days after the service of the request, except that a defendant may serve a response within 45 days after service of the summons and complaint upon that defendant. The court may allow a shorter or longer time. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, in which event the reasons for objection shall be stated. If objection is made to part of an item or category, the part shall be specified. In addition to other bases for objection, the response may state an objection to production of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. The response may also state an objection to a requested form for producing electronically stored information. If the responding party objects to a requested form, or if no form is specified in the request, the party must state the form or forms it intends to use. The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested.

Unless otherwise stipulated by the parties or ordered by the court, the following procedures apply to producing documents or electronically stored information:
(1) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;
(2) If a request does not specify a form for producing the electronically stored information, a party must produce it in a reasonably usable form or forms; and
(3) A party need not produce the same electronically stored information in more than one form.

(b1) Form of response. There shall be sufficient space following each request in which the respondent may state the response. The respondent shall: (1) state the response in the space provided, using additional pages if necessary; or (2) restate the request to be followed by the response. An objection to a request shall be made by stating the objection and the reason therefore either in the space following the request or following the restated request.

(c) Persons not parties. – This rule does not preclude an independent action against a person not a party for production of documents and things and permission to enter upon land. (1967, c. 954, s. 1; 1969, c. 895, s. 8; 1973, c. 923, s. 1; 1975, c. 762, s. 2; 1987, c. 613, s. 2; 2011 199, s. 4.)

G.S. § 8C: Evidence Code

- G.S. § 8C-10 Rule 1001. Definitions.
- G.S. § 8C-10 Rule 1002. Requirement of original.
- G.S. § 8C-10 Rule 1003. Admissibility of duplicates.
- G.S. § 8C-10 Rule 1004. Admissibility of other evidence of contents.
- G.S. § 8C-10 Rule 1005. Public records.
- G.S. § 8C-10 Rule 1006. Summaries.
- G.S. 8C-10 Rule 1007. Testimony or written admission of party.
- G.S. 8C-10 Rule 1008. Functions of court and jury.

G.S. § 8C-10 Rule 1001. Definitions.
For the purposes of this Article the following definitions are applicable:
(1) Writings and Recordings. – "Writings" and "recordings" consist of letters, words, sounds, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.

(2) Photographs. – "Photographs" include still photographs, x ray films, video tapes, and motion pictures.
(3) Original. – An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."
(4) Duplicate. – A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduce the original. (1983, c. 701, s. 1.)

G.S. § 8C-10 Rule 1002. Requirement of original.
To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by statute. (1983, c. 701, s. 1.)

G.S. § 8C-10 Rule 1003. Admissibility of duplicates.
A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original. (1983, c. 701, s. 1.)

G.S. § 8C-10 Rule 1004. Admissibility of other evidence of contents.
The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if:
(1) Originals Lost or Destroyed. – All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or
(2) Original Not Obtainable. – No original can be obtained by any available judicial process or procedure; or
(3) Original in Possession of Opponent. – At a time when an original was under the control of a party against whom offered, he was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and he does not produce the original at the hearing; or
(4) Collateral Matters. – The writing, recording, or photograph is not closely related to a controlling issue. (1983, c. 701, s. 1.)

G.S. § 8C-10 Rule 1005. Public records.

The contents of an official record, or of a document authorized to be recorded or filed and actually recorded or filed, including data compilations in any form, if otherwise admissible, may be proved by copy, certified as correct in accordance with Rule 902 or testified to be correct by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given. (1983, c. 701, s. 1.)

G.S. § 8C-10 Rule 1006. Summaries.

The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at a reasonable time and place. The court may order that they be produced in court. (1983, c. 701, s. 1.)

G.S. § 8C-10 Rule 1007. Testimony or written admission of party.

Contents of writings, recordings, or photographs may be proved by the testimony or deposition of the party against whom offered or by his written admission, without accounting for the nonproduction of the original. (1983, c. 701, s. 1.)

G.S. § 8C-10 Rule 1008. Functions of court and jury.

When the admissibility of other evidence of contents of writings, recordings, or photographs under these rules depends upon the fulfillment of a condition of fact, the question whether the condition has been fulfilled is ordinarily for the court to determine in accordance with the provisions of Rule 104. However, when an issue is raised (a) whether the asserted writing ever existed, or (b) whether another writing, recording, or photograph produced at the trial is the original, or (c) whether other evidence of contents correctly reflects the contents, the issue is for the trier of fact to determine as in the case of other issues of fact. (1983, c. 701, s. 1.)

Appendix B: Electronic Records Policy and Self-Warranty

- Purpose of Policy and Self-Warranty
- Limitation of Self-Warranty
- Responsibility for Ensuring Integrity of Electronic Records
- Model Policy and Self-Warranty

Purpose of Policy and Self-Warranty. The increased complexity of safeguarding the integrity of public records produced by information technology requires greater attention to issues relating to security, accuracy, reliability, and accountability. The Electronic Records Policy and Self-Warranty is designed to be used as a self-evaluation tool to ensure that electronic records produced by state, county, and municipal agencies are able to be retained for the designated retention period, and are created, reproduced, and otherwise managed in accordance with these guidelines and with other guidance produced by the Department of Cultural Resources.

State agencies should use the self-warranty form when using electronic formats to store records classified as "permanent" or which have retention periods of at least ten years in the records retention schedule. Local agencies should use the self-warranty form when converting paper records into electronic formats. Every state and local agency should maintain an electronic records policy in-office signed by the records custodian and by an IT professional or other project supervisor. The model policy provided here should be adapted to suit the electronic records management practices of the individual agency. The agency's records analyst may be contacted for assistance in developing a policy. All staff should be made aware of this policy and be trained on it.

Policies developed by a local agency should include a third component, a Request for Disposal of Original Records Duplicated by Electronic Means form. This form is used to request approval from the Department of Cultural Resources to dispose of paper records which have been scanned, entered into databases, or otherwise duplicated through digital imaging or other conversion to a digital environment.

Limitation of Self-Warranty. The self-warranting of records in itself does not authorize the destruction of records, originals or copies, nor does it change current records retention and disposition scheduling procedures.

Responsibility for Ensuring Integrity of Electronic Records. The government agency producing electronic records and/or reproductions is responsible for ensuring the records' authenticity and

accuracy. The Department of Cultural Resources is not responsible for certifying the authenticity or accuracy of any records, whether originals or reproductions, produced by the originating agency.

Model policy and Self-Warranty form. A model policy, which includes the self-warranty form is available on the State Archives website (**www.ncdcr.gov/archives**) under the "For Government" tab.